

Kombinasi Algoritma Hill Cipher menggunakan Kode Telpo Wilayah Jawa Tengah dengan Tabel Sin

Aditya Hastami Ruger

Magister Teknik Informatika, Universitas Amikom Yogyakarta Jl. Ring Road Utara,
Yogyakarta, Tlp (0274) 884201

e-mail: aditya.ruger@students.amikom.ac.id

Abstrak

Media komunikasi mudah diakses oleh semua orang. Dengan bebasnya orang lain menggunakan media komunikasi, memberikan dampak bagi keamanan informasi. Dengan rentannya keamanan informasi, informasi dapat diubah atau di hack oleh orang yang tidak bertanggung jawab. Untuk itu agar informasi tidak dapat di ubah oleh orang lain, maka ada alternatif cara untuk menyamarkan pesan yang terkandung dalam informasi tersebut yaitu menggunakan kriptografi, salah satu metode nya dengan Hill Cipher, yaitu suatu metode untuk menyamarkan pesan yang terdapat di dalam informasi tersebut. Metode Hill Cipher tersebut dikombinasikan dengan kode telepon wilayah Jawa Tengah dan diubah dengan tabel sin. Tujuan dari penelitian ini yaitu mengenkripsi pesan yang terkandung dalam informasi menggunakan metode Hill Cipher yang dikombinasikan dengan kode telepon wilayah Jawa Tengah dan tabel sin.

Kata kunci— Hill Cipher, Kriptografi, Kode telepon

1. PENDAHULUAN

Perkembangan teknologi informasi sangat pesat, sehingga media komunikasi mudah diakses oleh semua orang. Dengan bebas nya akses media informasi di media internet, memberikan dampak bagi keamanan informasi. Dengan rentannya keamanan suatu informasi, informasi tersebut dapat diubah atau dihapus isinya oleh orang lain, sehingga pesan yang dikirim rusak ketika sampai tujuan. Untuk itu agar pesan yang dikirim aman dan tidak rusak maka pesan tersebut harus disamarkan atau disembunyikan agar orang lain tidak bisa melihat informasi yang terdapat didalam pesan tersebut. Cara untuk menyamarkan suatu pesan menggunakan kriptografi.

Kriptografi merupakan ilmu yang mempelajari untuk menyembunyikan suatu pesan agar pesan yang dikirim ke tempat tujuan tidak mudah dibaca oleh orang yang tidak berkewajiban untuk membaca pesan tersebut. Fungsi dari kriptografi yaitu menyembunyikan informasi penting yang terdapat didalam pesan, atau dengan kata lain memberi sandi kedalam pesan yang dikirim. Dengan diberinya sandi, pesan tersebut aman sampai tujuan.

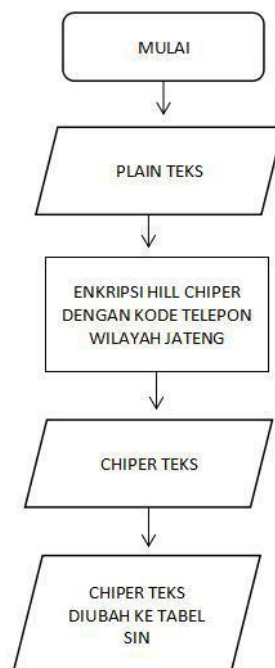
Beberapa penelitian di bidang kriptografi penelitian Yuningrat Dwi Putri, Rosihan, Salkin Lutfi, judul penelitian Penerapan Kriptografi Caesar Cipher Pada Fitur Chating Sistem Informasi Freelance [1]. Metode penelitian dengan cara pengumpulan data dan fitur chat pada sistem informasi freelance. Algoritma yang digunakan caesar cipher. Kesimpulan dari penelitian tersebut adalah pembuatan fitur chat pada sistem freelance bisa menggunakan pemrograman PHP. Penelitian Selviana Yunita, Patmawati Hasan, dengan judul penelitian Modifikasi Algoritma Hill Cipher dan Twofish menggunakan metode kode wilayah telepon [2]. Metode penelitian menggunakan Hill Cipher dan Twofish. Kesimpulan dari penelitian tersebut adalah dengan melalui modifikasi algoritma hill cipher dan twofish, proses enkripsi dan dekripsi file sangat bergantung dengan besarnya ukuran file, dimana ukuran file akan

mempengaruhi kecepatan dan jumlah data yang diproses. Semakin besar ukuran file, maka akan semakin lama proses enkripsi dan dekripsinya. Penelitian Helmi Sahara. Judul penelitian Implementasi Pengamanan Pesan Chatting menggunakan Metode Vignere Chiper dan Chiper Block Chaining [3]. Metode penelitian menggunakan Vignere Chiper dan Chiper Block Chaining. Kesimpulan dari penelitian tersebut Pentingnya melakukan pengamanan pesan chatting, agar terhindar dari pihak-pihak yang ingin merusak. Penelitian Gede Angga Pradipta. Judul penelitian Penerapan Kombinasi Metode Enkripsi Vignere Chiper dan Transposisi pada Aplikasi Client Server Chatting [4]. Metode penelitian menggunakan Vignere Chiper. Kesimpulan dari penelitian yaitu Implementasi program enkripsi data dengan metode vigenere dan transposisi dapat meningkatkan keamanan pengiriman pesan ke server. Penelitian Pratiwi Rahmadi dengan Judul penelitian Penyandian Teks dengan Metode Hill Chiper [5]. Metode penelitian menggunakan Hill Chiper. Kesimpulan dari penelitian Pada kriptografi, proses menyandikan text (*password*) dilakukan dengan metode Hill berjalan dengan baik untuk 6 digit angka pada PIN (Personal Identifier Number) yang diberikan oleh bank kepada nasabahnya. Implementasi cipher hills pada kode ASCII memberikan kemungkinan yang luas pada lebih banyak karakter yang tercakup, tidak hanya terbatas pada 26 alfabet, tetapi juga mencakup karakter-karakter lain. Penelitian Rudiyanto dan Safrina Amini dengan judul penelitian Implementasi Kriptografi Untuk Pengamanan Pesan Teks Pada Aplikasi Chatting Berbasis Android Dengan Metode Vigenere Cipher Pada Smk Negeri 7 Kota Tangerang [6]. Metode penelitian menggunakan Vignere Chiper. Kesimpulan dari penelitian Mempermudah guru dan wali murid untuk menyampaikan suatu pesan, sehingga bisa mengetahui perkembangan anaknya disekolah secara tak langsung.

2. METODE PENELITIAN

2.1 Alur Penelitian

Alur penelitian yang digunakan untuk kombinasi Hill Chiper dengan kode pos wilayah Jawa Tengah yang dapat dilihat pada gambar 1.



Gambar 1 Alur Penelitian

Penjelasan dari alur tersebut yaitu pertama menginput *plaintext*, lalu setelah menginput *plaintext* maka akan diproses enkripsi menggunakan *hill chiper* dengan kombinasi metode kode telepon wilayah jawa tengah, dan setelah proses enkripsi selesai maka akan mendapatkan hasil *chipper* teksnya.

2. 2 Hill Chiper

Hill chiper merupakan algoritma kriptografi yang menggunakan *polyalphabeti* yang menggunakan perhitungan matriks. Kunci pada *Hill Chiper* yaitu matriks K yang berukuran $n \times n$ yang digunakan untuk melakukan substitusi terhadap n alfabet.

2. 3 Kode Telepon Wilayah Jawa Tengah

Kode telepon tersebut menggunakan wilayah Jawa Tengah yang akan ditampilkan pada gambar 2.

KODE TELEPON	DESA	MODIFIKASI
0271	SOLO	4271
0281	PURWOKERTO	4281
0273	WONOGIRI	4273
0283	TEGAL	4283
0284	PEMALANG	4284
0286	WONOSOBO	4286
0291	DEMAK	4291
0293	MAGELANG	4293
0298	SALATIGA	4298
0274	YOGYAKARTA	4274

Gambar 2 Kode Telepon Wilayah Jawa Tengah

2. 4 Tabel Sin

TABEL SINUS, COSINUS, DAN TANGEN															
α	sin α	cos α	tan α	α	sin α	cos α	tan α	α	sin α	cos α	tan α	α	sin α	cos α	tan α
0°	0,000	1,000	0,000	45°	0,707	0,707	1,000	90°	1,000	0,000	∞	135°	0,707	-0,707	-1,000
1°	0,017	0,999	0,017	46°	0,719	0,695	1,036	91°	0,999	-0,017	-0,017	136°	0,695	-0,719	-1,066
2°	0,035	0,999	0,035	47°	0,731	0,682	1,072	92°	0,999	-0,035	-0,035	137°	0,682	-0,731	-1,093
3°	0,052	0,999	0,052	48°	0,743	0,669	1,111	93°	0,999	-0,052	-0,052	138°	0,669	-0,743	-1,120
4°	0,070	0,998	0,070	49°	0,755	0,656	1,150	94°	0,998	-0,070	-0,070	139°	0,656	-0,755	-1,149
5°	0,087	0,998	0,087	50°	0,766	0,643	1,192	95°	0,998	-0,087	-0,087	140°	0,643	-0,766	-1,179
6°	0,105	0,995	0,105	51°	0,777	0,629	1,235	96°	0,995	-0,105	-0,105	141°	0,629	-0,777	-1,210
7°	0,122	0,993	0,123	52°	0,788	0,616	1,280	97°	0,993	-0,122	-0,122	142°	0,616	-0,788	-1,241
8°	0,139	0,990	0,141	53°	0,799	0,602	1,327	98°	0,990	-0,139	-0,139	143°	0,602	-0,799	-1,273
9°	0,156	0,988	0,158	54°	0,809	0,588	1,376	99°	0,988	-0,156	-0,156	144°	0,588	-0,809	-1,306
10°	0,174	0,985	0,176	55°	0,819	0,574	1,428	100°	0,985	-0,174	-0,174	145°	0,574	-0,819	-1,340
11°	0,191	0,982	0,194	56°	0,829	0,559	1,483	101°	0,982	-0,191	-0,191	146°	0,559	-0,829	-1,375
12°	0,208	0,978	0,213	57°	0,839	0,545	1,540	102°	0,978	-0,208	-0,208	147°	0,545	-0,839	-1,411
13°	0,225	0,974	0,231	58°	0,848	0,530	1,600	103°	0,974	-0,225	-0,225	148°	0,530	-0,848	-1,448
14°	0,242	0,970	0,249	59°	0,857	0,515	1,664	104°	0,970	-0,242	-0,242	149°	0,515	-0,857	-1,486
15°	0,259	0,966	0,268	60°	0,866	0,500	1,732	105°	0,966	-0,259	-0,259	150°	0,500	-0,866	-1,525
16°	0,276	0,961	0,287	61°	0,875	0,485	1,804	106°	0,961	-0,276	-0,276	151°	0,485	-0,875	-1,565
17°	0,292	0,956	0,306	62°	0,883	0,469	1,881	107°	0,956	-0,292	-0,292	152°	0,469	-0,883	-1,606
18°	0,309	0,951	0,325	63°	0,891	0,454	1,963	108°	0,951	-0,309	-0,309	153°	0,454	-0,891	-1,648
19°	0,326	0,946	0,344	64°	0,899	0,438	2,050	109°	0,946	-0,326	-0,326	154°	0,438	-0,899	-1,691
20°	0,342	0,940	0,364	65°	0,906	0,423	2,145	110°	0,940	-0,342	-0,342	155°	0,423	-0,906	-1,735
21°	0,358	0,934	0,384	66°	0,914	0,407	2,246	111°	0,934	-0,358	-0,358	156°	0,407	-0,914	-1,780
22°	0,375	0,927	0,404	67°	0,921	0,391	2,356	112°	0,927	-0,375	-0,375	157°	0,391	-0,921	-1,826
23°	0,391	0,921	0,424	68°	0,927	0,375	2,475	113°	0,921	-0,391	-0,391	158°	0,375	-0,927	-1,874
24°	0,407	0,914	0,445	69°	0,934	0,358	2,605	114°	0,914	-0,407	-0,407	159°	0,358	-0,934	-1,923
25°	0,423	0,906	0,466	70°	0,940	0,342	2,747	115°	0,906	-0,423	-0,423	160°	0,342	-0,940	-1,974
26°	0,438	0,899	0,488	71°	0,946	0,326	2,904	116°	0,899	-0,438	-0,438	161°	0,326	-0,946	-2,026
27°	0,454	0,891	0,510	72°	0,951	0,309	3,078	117°	0,891	-0,454	-0,454	162°	0,309	-0,951	-2,080
28°	0,469	0,883	0,532	73°	0,956	0,292	3,271	118°	0,883	-0,469	-0,469	163°	0,292	-0,956	-2,136
29°	0,485	0,875	0,554	74°	0,961	0,276	3,487	119°	0,875	-0,485	-0,485	164°	0,276	-0,961	-2,193
30°	0,500	0,866	0,577	75°	0,966	0,259	3,732	120°	0,866	-0,500	-0,500	165°	0,259	-0,966	-2,251
31°	0,515	0,857	0,601	76°	0,970	0,242	4,011	121°	0,857	-0,515	-0,515	166°	0,242	-0,970	-2,311
32°	0,530	0,848	0,625	77°	0,974	0,225	4,331	122°	0,848	-0,530	-0,530	167°	0,225	-0,974	-2,373
33°	0,545	0,839	0,649	78°	0,978	0,208	4,705	123°	0,839	-0,545	-0,545	168°	0,208	-0,978	-2,437
34°	0,559	0,829	0,675	79°	0,982	0,191	5,145	124°	0,829	-0,559	-0,559	169°	0,191	-0,982	-2,503
35°	0,574	0,819	0,700	80°	0,985	0,174	5,671	125°	0,819	-0,574	-0,574	170°	0,174	-0,985	-2,571
36°	0,588	0,809	0,727	81°	0,988	0,156	6,314	126°	0,809	-0,588	-0,588	171°	0,156	-0,988	-2,641
37°	0,602	0,799	0,754	82°	0,990	0,139	7,115	127°	0,799	-0,602	-0,602	172°	0,139	-0,990	-2,714
38°	0,616	0,788	0,781	83°	0,993	0,122	8,144	128°	0,788	-0,616	-0,616	173°	0,122	-0,993	-2,790
39°	0,629	0,777	0,810	84°	0,995	0,105	9,514	129°	0,777	-0,629	-0,629	174°	0,105	-0,995	-2,869
40°	0,643	0,766	0,839	85°	0,996	0,087	11,430	130°	0,766	-0,643	-0,643	175°	0,087	-0,996	-2,951
41°	0,656	0,755	0,869	86°	0,998	0,070	14,301	131°	0,755	-0,656	-0,656	176°	0,070	-0,998	-3,036
42°	0,669	0,743	0,900	87°	0,999	0,052	19,081	132°	0,743	-0,669	-0,669	177°	0,052	-0,999	-3,124
43°	0,682	0,731	0,933	88°	0,999	0,035	28,636	133°	0,731	-0,682	-0,682	178°	0,035	-0,999	-3,215
44°	0,695	0,719	0,966	89°	1,000	0,017	57,290	134°	0,719	-0,695	-0,695	179°	0,017	-1,000	-3,309
45°	0,707	0,707	1,000	90°	1,000	0,000	∞	135°	0,707	-0,707	-1,000	180°	0,000	-1,000	0,000

Gambar 3 Tabel Sin

3. HASIL DAN PEMBAHASAN

3.1 Modifikasi Hill Chiper

Mengenkripsi plainteks “Semoga Pandemi Virus Corona Cepat Berakhir“. Dengan menggunakan matriks kode telepon wilayah Jawa Tengah dengan kunci, yang akan ditampilkan pada gambar 4 sebagai berikut.

K1	7	4
	1	2
K2	8	4
	1	2
K3	7	4
	3	2
K4	8	4
	3	2
K5	8	4
	4	2
K6	8	4
	6	2
K7	9	4
	1	2
K8	9	4
	3	2
K9	9	4
	8	2

Gambar 4 Kunci Enkripsi

Langkah penyelesaiannya pertama ubah dulu huruf ke angka terlebih dahulu, yang akan ditampilkan pada gambar 5.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Gambar 5 Deret Huruf dan Angka

Angka Gambar dibawah plainteks yang sudah diubah ke angka.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
S	18	M	12	G	6	P	15	N	13	E	4	I	8
E	4	O	14	A	0	A	0	O	3	M	12	K	10
15	16	17	18	19									
A	0	B	1	R	17	K	10	I	8				
T	19	E	4	A	0	H	7	R	17				

Gambar 6 Plaintext yang telah diubah ke Angka

Maka didapatkan *plainteks* “Semoga Pandemi Virus Corona Cepat Berakhir“ yang diubah ke angka yaitu sebagai berikut :

“8,4,12,14,6,0,15,0,13,3,4,12,8,10,21,8,17,20,18,2,14,17,14,13,0,2,4,15,0,19,1,4,17,0,10,7,8,17“

Berikut hasil *chiperteks* yang akan di *enkripsi* menggunakan *hill chiper* yang akan ditampilkan pada gambar 7.

1	7	4	18	$7*18+4*4$	142	12	0,342	11	7	4	14	$7*14+4*17$	187	5	0,087
	1	2	4	$1*18+2*4$	26	0	0		1	2	17	$1*14+2*17$	48	22	0,375
2	8	4	12	$8*12+4*14$	152	22	0,375	12	8	4	14	$8*14+4*13$	164	8	0,139
	1	2	14	$1*12+2*14$	40	14	0,242		1	2	13	$1*14+2*13$	40	14	0,242
3	7	4	6	$7*6+4*0$	42	16	0,276	13	7	4	0	$7*0+4*2$	8	8	0,139
	3	2	0	$3*6+2*0$	18	18	0,309		3	2	2	$3*0+2*2$	4	4	0,07
4	8	4	15	$8*15+4*0$	120	16	0,276	14	8	4	4	$8*4+4*15$	92	14	0,242
	3	2	0	$3*15+2*0$	45	19	0,326		3	2	15	$3*4+2*15$	42	16	0,276
5	8	4	13	$8*13+4*3$	116	12	0,208	15	8	4	0	$8*0+4*19$	76	24	0,407
	4	2	3	$4*13+2*3$	58	6	0,105		4	2	19	$4*0+2*19$	38	12	0,208
6	8	4	4	$8*4+4*12$	80	2	0,035	16	8	4	1	$8*1+4*4$	24	24	0,407
	6	2	12	$6*4+2*12$	48	22	0,375		6	2	4	$6*1+2*4$	14	14	0,242
7	9	4	8	$9*8+4*10$	112	8	0,139	17	9	4	17	$9*17+4*0$	153	23	0,391
	1	2	10	$1*8+2*10$	28	2	0,035		1	2	0	$1*17+2*0$	17	17	0,292
8	9	4	21	$9*21+4*8$	221	13	0,225	18	9	4	10	$9*10+4*7$	118	14	0,242
	3	2	8	$3*21+2*8$	79	1	0,017		3	2	7	$3*10+2*7$	44	18	0,309
9	9	4	17	$9*17+4*20$	233	25	0,423	19	9	4	8	$9*8+4*17$	140	10	0,174
	8	2	20	$8*17+2*20$	176	20	0,342		8	2	17	$8*8+2*17$	98	20	0,342
10	7	4	18	$7*18+4*2$	194	12	0,208								
	4	2	2	$4*18+2*2$	76	24	0,407								

Gambar 7 Enkripsi *Hill Chiper*

Hasil *Chiper text* telah diubah dengan tabel *sin* dapat dilihat pada gambar 8.

12	0,342	5	0,087
0	0	22	0,375
22	0,375	8	0,139
14	0,242	14	0,242
16	0,276	8	0,139
18	0,309	4	0,07
16	0,276	14	0,242
19	0,326	16	0,276
12	0,208	24	0,407
6	0,105	12	0,208
2	0,035	24	0,407
22	0,375	14	0,242
8	0,139	23	0,391
2	0,035	17	0,292
13	0,225	14	0,242
1	0,017	18	0,309
25	0,423	10	0,174
20	0,342	20	0,342
12	0,208		
24	0,407		

Gambar 8. Hasil *Chiper Text*

4. KESIMPULAN

Algoritma *Hill Chiper* bisa dikombinasikan dengan kode telepon wilayah Jawa Tengah dan dari *chipertext* nya diubah ke tabel *sin*.

5. SARAN

Dalam penelitian selanjutnya dapat diimplementasikan algoritma *Hill Cipher* menggunakan kode telepon wilayah Jawa Tengah, dan dapat ditambahkan algoritma yang lain Aplikasi dapat dimasukan ke dalam file mp3, dan gambar.

DAFTAR PUSTAKA

- [1] Hidayat, M. H., Gerhana, Y. A., & Syaripudin, U. 2018. Kombinasi Algoritma Kriptografi Vigenere Cipher dan Hill Cipher untuk Penyandian Pesan Rahasia pada Metode Steganografi, vol 1, hal 125–131.
 - [2] Dony Ariyus, 2008, Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi, Andi Offset.
 - [3] Suyanto M, “Pengantar Teknologi Informasi” ,Penerbit ANDI, Yogyakarta, 2015
 - [4] Dony Ariyus dan Rum Andri K.R, “Komunikasi Data”, Penerbit ANDI, Yogyakarta, 2008
 - [5] Rinaldi Munir, “Kriptografi”, Penerbit Informatika, Bandung, 2006.
 - [6] Muhammad Azzam Mujaddid, 2017, “ Implementasi Algoritma Hill Cipher dengan Modifikasi Proses Menggunakan Algoritma Caesar Cipher pada File Dokumen Plaintext”.
 - [7] Akik Hidayat & Tuty Alawiyah, 2013, “ Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang “.
 - [8] Selviana Yunita, Patmawati Hasan, Dony Ariyus, 2019, “ Algoritma Hill Cipher dan Twofish menggunakan Kode Wilayah Telepon “.
 - [9] Dewi Sartika Ginting, 2017, “ Kriptografi Simetris dengan Kombinasi Hill Cipher dan Affine Cipher di dalam Matriks Cipher Transposisi dengan Menerapkan Pola Alur Bajak Sawah “.
 - [10] Ardiansyah Rifky, “ Pengembangan Algoritma Vigenere Cipher Menggunakan Metode Pergeseran kunci Berbasis Biner “.
-